

-65-

CLAIMS

5

1. A method of transmitting contents,
which are to be received at a reception side where a
portion of the contents is previewed while the
contents are not accessible for playing other than
10 for a preview purpose, comprising the steps of:
 encrypting the contents by a first
 encryption key;
 generating information indicative of an
 elapsed time of the contents that indicates a
15 relationship between positions on a time axis of the
 contents representing an amount of time that passes
 as the contents are played and a time count that
 accrues as a preview time when the contents are
 previewed;
20 encrypting the first encryption key and
 the information indicative of an elapsed time of the
 contents by a second encryption key, thereby
 generating first encrypted information;
 encrypting the second encryption key and
25 content-usage control information by a third
 encryption key, thereby generating second encrypted
 information, said content-usage control information
 indicating usage of the contents on the reception
 side; and
30 transmitting the encrypted contents, the
 first encrypted information, and the second
 encrypted information to the reception side.

-66-

2. An apparatus for transmitting contents, which are to be received at a reception side where a portion of the contents is previewed while the contents are not accessible for playing other than for a preview purpose, comprising the steps of:

5 a content encrypting unit which encrypts the contents by a first encryption key;

a content-transmission controlling unit which generates information indicative of an elapsed time of the contents that indicates a relationship

10 between positions on a time axis of the contents representing an amount of time that passes as the contents are played and a time count that accrues as a preview time when the contents are previewed;

15 a first encrypting unit which encrypts the first encryption key and the information indicative of an elapsed time of the contents by a second encryption key, thereby generating first encrypted information;

20 a second encrypting unit which encrypts the second encryption key and content-usage control information by a third encryption key, thereby generating second encrypted information, said content-usage control information indicating usage

25 of the contents on the reception side; and

a transmission unit which transmits the encrypted contents, the first encrypted information, and the second encrypted information to the reception side.

30

-67-

3. The apparatus as claimed in claim 2,
wherein said content-transmission control unit
generates the information indicative of an elapsed
time of the contents such that said time count
5 linearly corresponds to said time axis of the
contents.

10

4. The apparatus as claimed in claim 2,
wherein said content-transmission control unit
generates the information indicative of an elapsed
time of the contents such that said time count is
15 not evenly assigned to the said time axis of the
contents.

20

5. The apparatus as claimed in claim 2,
wherein said content-transmission control unit
generates the information indicative of an elapsed
time of the contents such that said time count
25 decreases with passage of time on a portion of said
time axis of the contents, and increases with
passage of time on another portion of said time axis
of the contents.

30

6. The apparatus as claimed in claim 2,

-68-

wherein a preview-purpose content is attached to the contents at a start of the contents.

5

7. The apparatus as claimed in claim 2, wherein the content-usage control information includes a purchase flag for indicating whether the contents are purchased or rented on the reception side, said purchase flag being returned from the reception side for confirmation of a payment of a fee for the contents.

15

8. The apparatus as claimed in claim 2, wherein said transmission unit transmits the second encrypted information separately from the encrypted contents and the first encrypted information in response to a request from the reception side.

25

9. A machine-readable medium having a program embodied therein for causing a computer to transmit contents, which are to be received at a reception side where a portion of the contents is previewed while the contents are not accessible for playing other than for a preview purpose, said program comprising:

-69-

a content encrypting unit which encrypts the contents by a first encryption key;

a content-transmission controlling unit which generates information indicative of an elapsed time of the contents that indicates a relationship between positions on a time axis of the contents representing an amount of time that passes as the contents are played and a time count that accrues as a preview time when the contents are previewed;

10 a first encrypting unit which encrypts the first encryption key and the information indicative of an elapsed time of the contents by a second encryption key, thereby generating first encrypted information;

15 a second encrypting unit which encrypts the second encryption key and content-usage control information by a third encryption key, thereby generating second encrypted information, said content-usage control information indicating usage of the contents on the reception side; and

20 a transmission unit which transmits the encrypted contents, the first encrypted information, and the second encrypted information to the reception side.

25

10. A method of controlling encrypted contents that are received from a transmission side, wherein a portion of the encrypted contents is previewed while the encrypted contents are not accessible for playing other than for a preview

-70-

purpose, comprising the steps of:

separating received contents into the encrypted contents, first encrypted information, and second encrypted information, the first encrypted
5 information including a first encryption key and information indicative of an elapsed time of contents as encrypted by a second encryption key, and the second encrypted information including the second encryption key and content-usage control
10 information as encrypted by a third encryption key;

storing the encrypted contents and the first encrypted information in storage;

decoding the second encrypted information by the third encryption key so as to obtain the
15 second encryption key and the content-usage control information;

decoding the first encrypted information stored in the storage by the obtained second encryption key so as to obtain the first encrypted
20 key and the information indicative of an elapsed time of contents;

checking whether a preview of said portion of the encrypted contents is permitted based on the information indicative of an elapsed time of
25 contents and the content-usage control information; and

decoding said portion of the encrypted contents by the first encrypted key in response to a check result that a preview of said portion of the
30 encrypted contents is permitted,

wherein the information indicative of an elapsed time of contents indicates a relationship between positions on a time axis of contents

-71-

representing an amount of time that passes as the contents are played and a time count that accrues as a preview time when the contents are previewed.

5

11. An apparatus for controlling encrypted contents that are received from a transmission side, wherein a portion of the encrypted contents is previewed while the encrypted contents are not accessible for playing other than for a preview purpose, comprising:

a separating unit which separates received contents into the encrypted contents, first encrypted information, and second encrypted information, the first encrypted information including a first encryption key and information indicative of an elapsed time of contents as encrypted by a second encryption key, and the second encrypted information including the second encryption key and content-usage control information as encrypted by a third encryption key;

a content storage unit which stores the encrypted contents and the first encrypted information in storage;

a first decoding unit which decodes the second encrypted information by the third encryption key so as to obtain the second encryption key and the content-usage control information;

a second decoding unit which decodes the first encrypted information stored in the storage by the obtained second encryption key so as to obtain

-72-

the first encrypted key and the information
indicative of an elapsed time of contents;

a check unit which checks whether a
preview of said portion of the encrypted contents is
5 permitted based on the information indicative of an
elapsed time of contents and the content-usage
control information; and

a content decoding unit which decodes said
portion of the encrypted contents by the first
10 encrypted key in response to a check result that a
preview of said portion of the encrypted contents is
permitted,

wherein the information indicative of an
elapsed time of contents indicates a relationship
15 between positions on a time axis of contents
representing an amount of time that passes as the
contents are played and a time count that accrues as
a preview time when the contents are previewed.

20

12. The apparatus as claimed in claim 11,
further comprising:

25 a playing-time counter unit which counts
the time count as said portion of the encrypted
contents is decoded for playing; and

a charging unit which charges a fee
commensurate with the time count counted by said
30 playing-time counter unit,

wherein said check unit compares the time
count with an authorized-preview time length defined
in the content-usage control information, and said

-73-

charging unit refrains from charging a fee until the time count exceeds the authorized-preview time length.

5

13. The apparatus as claimed in claim 12, wherein said playing-time counter unit counts the time count based on a continuation index that is provided to correspond to a unit time by which said first encryption key changes.

15

14. The apparatus as claimed in claim 12, wherein said check unit is provided inside a security module that protects information therein from external access such as to prevent reading of the information.

25

15. The apparatus as claimed in claim 14, wherein said charging unit is provided inside said security module, and generates content-history information by combining the time count counted by the playing-time counter unit with the content-usage control information, said content-history information being paired up with content IDs, which are assigned to respective contents.

30

-74-

5 16. The apparatus as claimed in claim 15,
further comprising an encrypting unit which encrypts
the content-history information and the second
encryption key by use of an inherent key kept inside
said security module if the check unit finds that
10 the time count is smaller than the authorized-
preview time length, the content-history information
and the second encryption key encrypted by said
encrypting unit being stored in said content storage
unit.

15

 17. The apparatus as claimed in claim 16,
20 wherein the second encrypted information is stored
in said content storage unit together with the
encrypted contents after encryption by said
encrypting unit.

25

 18. The apparatus as claimed in claim 12,
wherein said charging unit sends a notice to the
30 transmission side through a communication channel,
said notice indicating whether the encrypted
contents are purchased or rented.

-75-

19. The apparatus as claimed in claim 12,
5 wherein a request for the second encrypted
information is sent to the transmission side via a
communication channel if the second encrypted
information is not included in the received contents,
and a fee for the encrypted contents is charged when
10 said charging unit receives the second encrypted
information.

15

20. A machine-readable record medium
having a program embodied therein for causing a
computer to control encrypted contents that are
received from a transmission side, wherein a portion
20 of the encrypted contents is previewed while the
encrypted contents are not accessible for playing
other than for a preview purpose, said program
comprising:

a separating unit which separates received
25 contents into the encrypted contents, first
encrypted information, and second encrypted
information, the first encrypted information
including a first encryption key and information
indicative of an elapsed time of contents as
30 encrypted by a second encryption key, and the second
encrypted information including the second
encryption key and content-usage control information
as encrypted by a third encryption key;

-76-

a content storage unit which stores the encrypted contents and the first encrypted information in storage;

5 a first decoding unit which decodes the second encrypted information by the third encryption key so as to obtain the second encryption key and the content-usage control information;

10 a second decoding unit which decodes the first encrypted information stored in the storage by the obtained second encryption key so as to obtain the first encrypted key and the information indicative of an elapsed time of contents;

15 a check unit which checks whether a preview of said portion of the encrypted contents is permitted based on the information indicative of an elapsed time of contents and the content-usage control information; and

20 a content decoding unit which decodes said portion of the encrypted contents by the first encrypted key in response to a check result that a preview of said portion of the encrypted contents is permitted,

25 wherein the information indicative of an elapsed time of contents indicates a relationship between positions on a time axis of contents representing an amount of time that passes as the contents are played and a time count that accrues as a preview time when the contents are previewed.